What is claimed is:

1. A device authentication system in which a first device authenticates a second device,

wherein the first device comprises:

a transmission/reception section that transmits and receives information to/from the second device;

a first information holding section that holds first authentication information in a secure area; and

a decider that makes a decision on authentication,

the second device comprises:

a transmission/reception section that transmits and receives information to/from the first device;

a second information holding section that holds second authentication information;

an information acquirer that acquires third authentication information from outside of the second device; and

an authentication information generator which generates fourth authentication information from the second authentication information and the third authentication information, and outputs the fourth authentication information to the first device through the transmission/reception section, and

the decider makes a decision on conformity between the first authentication information and the fourth authentication information to authenticate the second

device.

2. The device authentication system according to claim 1, wherein the second authentication information is information specific to the second device.

3. The device authentication system according to claim 1, wherein the second authentication information is random information generated in the first device.

4. The device authentication system according to claim 3, wherein the second authentication information is updated whenever the authentication processing is performed, and according to update of the second authentication information, the first authentication information held in the first information holding section in the first device is updated.

5. The device authentication system according to claim 1, wherein when the first device does not hold the first authentication information, a device that performs mutual authentication with the first device acquires the fourth authentication information from the second device, and sets the first device for the first authentication information as initial setting.

6. The device authentication system according to claim 1, wherein the third authentication information is held in a device that performs mutual authentication with the first device, and is provided from the device to the second device in authentication processing.

7. A device authentication method in which a first

device authenticates a second device,

wherein the first device holds first authentication information in a secure area,

the second device that holds second authentication information generates fourth authentication information form the second authentication information and third authentication information provided from outside of the second device, and

the first device makes a decision on conformity between the first authentication information and the fourth authentication information to authenticate the second device.

8. A second device to be authenticated by a first device, comprising:

a transmission/reception section that transmits and receives information to/from the first device;

an information holding section that holds second authentication information;

an information acquirer that acquires third authentication information from outside of the second device; and

an authentication information generator which generates fourth authentication information from the second authentication information and the third authentication information, and outputs the fourth authentication information to the first device through the transmission/reception section.

9. The second device according to claim 8, wherein the transmission/reception section receives random information from the first device, and the authentication information generator encrypts the random information using the fourth authentication information to transmit to the first device through the transmission/reception section.

10. The second device according to claim 8, wherein the transmission/reception section receives the random information from the first device, and the authentication information generator encrypts the fourth authentication information using the random information to transmit to the first device through the transmission/reception section.

11. The second device according to claim 8, further comprising:

an update control section that controls update of information required for processing for authentication,

wherein after authentication from the first device succeeds, substituting for the second authentication information, the update control section stores in the information holding section the random information as new second authentication information, generates key information that is new authentication information from the third authentication information and the random information, and has the first device hold the key information through the transmission/reception section.

12. The second device according to claim 9, further comprising:

an update control section that controls update of information required for processing for authentication,

wherein after authentication from the first device succeeds, substituting for the second authentication information, the update control section stores in the information holding section the random information as new second authentication information, generates key information that is new authentication information from the third authentication information and the random information, and has the first device hold the key information through the transmission/reception section.

13. The second device according to claim 10, further comprising:

an update control section that controls update of information required for processing for authentication,

wherein after authentication from the first device succeeds, substituting for the second authentication information, the update control section stores in the information holding section the random information as new second authentication information, generates key information that is new authentication information from the third authentication information and the random information, and has the first device hold the key information through the transmission/reception section.

14. A first device that authenticates a second device,

comprising:

a transmission/reception section that transmits and receives information to/from the second device;

an information holding section that holds first authentication information in a secure area; and

a decider that makes a decision on conformity between the fourth authentication information received in the transmission/reception section and the first authentication information.

15. The first device according to claim 14, further comprising:

a random information generator that generates random information to transmit to the second device through the transmission/reception section,

wherein the decider decodes information received in the transmission/reception section using the first authentication information, and makes a decision on conformity between the decoded information and the random information.

16. The first device according to claim 14, further comprising:

a random information generator that generates random information to transmit to the second device through the transmission/reception section,

wherein the decider decodes information received in the transmission/reception section using the random information, and makes a decision on conformity between

the decoded information and the first authentication information.

17. The first device according to claim 14, wherein after authentication of the second device succeeds, substituting for the first authentication information, the information holding section holds key information that is new authentication information received in the transmission/reception section, as new first authentication information.

18. The first device according to claim 15, wherein after authentication of the second device succeeds, substituting for the first authentication information, the information holding section holds key information that is new authentication information received in the transmission/reception section, as new first authentication information.

19. The first device according to claim 16, wherein after authentication of the second device succeeds, substituting for the first authentication information, the information holding section holds key information that is new authentication information received in the transmission/reception section, as new first authentication information.

20. A program for having a computer, which is integrated into a second device to be authenticated by a first device, execute the procedures of:

generating fourth authentication information from

second authentication information that the second device holds and third authentication information acquired from outside of the second device;

requesting an issue of random information to the first device; and

encrypting the random information received from the first device using the fourth authentication information to output to the first device.